8 Data Privacy and Compliance Considerations for Remote Workforces

Best Practices

Here are 8 best practices to help ensure your organization’s IT security protects employee privacy while staying in compliance.

1. **Protection**
   - Implement converged security to protect the data.
   - Adequate is simply not enough and many regulations stipulate state-of-the-art as a requirement.

2. **Governance**
   - Provide transparent data use policies and controls and make your strategy an asset with your customers so they know their privacy is safe with you.

3. **Visibility**
   - In order to protect the data, you need to be able to see the data you have, where it goes, and who’s using it.
   - Your security must have visibility across the network and into the cloud.

4. **Access**
   - With many regulations putting the power back in the hands of the data owners, they have the right to see how and where data is being used and to be forgotten if requested. Access management provides the necessary and scalable, automated controls.

5. **Simplified global policy management**
   - A single point of management for multiple cloud apps sets regional policies across the right channels in the right locations.

6. **Response**
   - Be ready for the worst-case scenario: a data breach.
   - You need both the plans and tools in place to rapidly respond, remediate, and report.

7. **Personal privacy protection**
   - The remote work era requires powerful security to protect PII and customer data from theft or misuse.
   - But you must also protect and respect the privacy rights of your employees, and having a carefully architected deployment strategy from the start is key.

8. **Monitor international changes**
   - Make sure your security program accounts for U.S. and international privacy legislation and compliance that continues to evolve.

Sources

1. Gartner Survey, June 5, 2020
4. © 2021 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.

As compliance and privacy regulations continue to expand, evolve and reframe, the duty for organizations remains the same: To secure and respect the privacy of both their customers and their people.

To find out more, visit our guide: Protecting Your Critical Data

Learn More:

Learn more about U.S. State Privacy Law: https://iapp.org/resources/article/state-comparison-table/

Follow ongoing privacy legislation at https://iapp.org/news/privacy-tracker/

80% of companies plan to allow employees to work remotely some of the time according to a Gartner survey.

Gartner says 82% of companies plan to allow employees to work remotely some of the time. Gartner Survey, June 5, 2020.

Here are 8 best practices to help ensure your organization’s IT security protects employee privacy while staying in compliance.

Beyond GDPR: New and pending regional legislations

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Legislation</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>California, U.S.</td>
<td>CCPA</td>
<td>Effective January 2020</td>
</tr>
<tr>
<td>Brazil</td>
<td>LGPD</td>
<td>Effective September 2020</td>
</tr>
<tr>
<td>China</td>
<td>PIPL</td>
<td>Draft legislation released October 2020</td>
</tr>
<tr>
<td>Canada</td>
<td>Consumer Privacy Protection Act</td>
<td>Draft legislation released September 2020</td>
</tr>
<tr>
<td>Singapore</td>
<td>PDPA</td>
<td>Implementation February 2021</td>
</tr>
<tr>
<td>U.S.</td>
<td>Safe Data Act</td>
<td>September 2020 - This sponsored bill is the latest attempt to create a Federal Privacy law.</td>
</tr>
</tbody>
</table>

For more information, visit: forcepoint.com